USDA United States Department of Agriculture

Food Safety and Inspection Service

Volume 19 Number 13

FSIS Constituent Update

Jan. 15, 2016

Retail *Listeria monocytogenes* (*Lm*) Pilot Project Update

On Jan. 25, 2016, FSIS will launch a year-long nationwide pilot project to assess whether retailers are using the recommendations in the FSIS Best Practices Guidance for Controlling *Listeria monocytogenes* (*Lm)* in Retail Delicatessens, issued in June 2015 (FSIS Retail Lm Guideline). FSIS will not sample for *Lm* at retail as part of the pilot project. As part of the pilot project, FSIS Compliance Investigators will complete a questionnaire which will be used to assess practices in the following areas: product handling, cleaning and sanitizing, facility and equipment controls, and employee practices. FSIS will use the findings from the questionnaire to determine whether retailers are following the *Lm* control measures recommended in the FSIS Retail *Lm* Guideline. Compliance Investigators will discuss with retailers vulnerabilities that are observed during the survey, but FSIS will not be asking the retail operator to complete the survey.

FSIS performed a pre-pilot project at 16 retail establishments in various parts of the country the week of Dec. 8-15, 2015, to gather information to inform the nationwide pilot project. Preliminary findings from the pre-pilot project indicated that retailers were not aware of the FSIS Retail *Lm* Guideline, at least at the store level, and additional outreach is needed.

Continue on Page 2

Updates To Microbiology and Pathology Laboratory Guidebooks

Seven analytical methods published in the original 1998 Microbiology Laboratory Guidebook (MLG) are obsolete and no longer used by the USDA, FSIS Laboratories. The chapters which are no longer operative and that will be archived on Feb.15, 2016 include: MLG 7 (Aeromonas species), MLG 9 (Yersinia enterocolitica), MLG 11 (Enzymes), MLG 14 (Clostridium botulinum Toxins), MLG 16 (Agarose Thin-Layer Isoelectric Focusing Species Determination), MLG 18 (Species Identification Field Tests -SIFT) and MLG 19 (Chloramphenicol competitive Enzyme-Linked Immunoassay -CELIA). To review the guidebook, please visit h*ttp://www.fsis.usda.gov/wps/portal/fsis/topics/science/laboratories-and-procedures/guidebooks-and-methods/microbiology-laboratory-guidebook*.

The FSIS Pathology Laboratory Guidebook (PLG) will be updated to include two extraneous materials analysis chapters: PLG 0002.00 Rodent Adulteration and Infestation Sample Analysis and PLG 0003.00 Alkaline Phosphatase Test for Mammalian Fecal Material. FSIS intends to begin using the chapters on Feb.15, 2016. To review the guidebook, please visit *http://www.fsis.usda.gov/wps/portal/fsis/topics/science/laboratories-and-procedures/guidebooks-and-methods/pathology-laboratory-guidebook/pathology-laboratory-guidebook*.

In This Issue

Export Requirement Updates

The Library of Export Requirements has been updated for the following countries:

Israel
Jordan
People's Republic of China
Republic of Korea
Taiwan

For a complete list of countries, visit *http://www.fsis.usda.gov/wps/portal/fsis/topics/international-affairs/exporting-products*.

... Retail *Listeria*

Continued from Page 1

The pre-pilot also found that a higher percentage of retailers followed the facility and equipment controls and employee practices recommendations (94 and 83% respectively) than the product handling, and cleaning and sanitizing recommendations (65 and 63%, respectively).

FSIS will distribute a tri-fold brochure describing *Lm* control measures as part of its outreach activities during the pilot. FSIS will analyze the information from the pilot project on a quarterly basis and will post results of this analysis on the FSIS website. The Agency will announce the availability of this analysis through the *Constituent Update.* Once the data from the pilot program is analyzed, FSIS plans to seek input from the National Advisory Committee on Meat and Poultry Inspection (NACMPI) regarding next steps for *Lm* controls at retail.

Retailers can refer questions regarding the Lm pilot project to the Risk, Innovations, and Management Staff through askFSIS or by telephone at 1-800-233-3935. When submitting a question, use the 'Submit a Question tab' and enter "Retail *Lm*" in the subject field.

Reminder: FSIS to Hold Educational Meetings on Inspection of Siluriformes Fish

FSIS will be conducting educational meetings regarding the final rule, "Mandatory Inspection of Fish of the Order Siluriformes and Products Derived from Such Fish," published in the *Federal Register* on Dec. 2, 2015. The purpose of the meetings is to educate participants on the final rule, as well as on what will be expected of domestic operations before and after the rule becomes effective on March 1, 2016. There will be a question and answer period following the presentation.

The final rule may be accessed from the FSIS website at *http://www.fsis.usda.gov/wps/portal/fsis/topics/inspection/siluriformes*.

The first meeting is open for all stakeholders and will be held Jan. 21, 2016, from 1:00 pm - 4:00 pm ET in Washington, DC at Patriots Plaza III, 355 E Street, SW, in the main floor auditorium. All persons wishing to attend are strongly encouraged to register in advance and allocate extra time to get through security screening. On-site registration will begin at 12:30 pm.

A second meeting for all stakeholders will be held on Jan. 27, 2016, from 1:00 pm - 4:00 pm CT in Stoneville, MS at the Charles W. Capps Jr. Entrepreneurial Center, Delta Research and Extension Center, Mississippi State University, 82 Stoneville Road, Stoneville, MS 38776. All persons wishing to attend are encouraged to register in advance and allocate extra time to get through security screening. FSIS will announce information for future Siluriformes fish educational meetings in subsequent *Constituent Updates.*

To pre-register for any of the meetings, please go to *http://www.fsis.usda.gov/wps/portal/fsis/newsroom/meetings.* For more information or special accommodations, please contact Evelyn Gomez at 202-418-8903 or evelyn.gomez@fsis.usda.gov.

We Want to Hear From You

The *Constituent Update* Content and Technical Review Committee seeks feedback from its readers. Please let us know what you think about the *Constituent Update* and send comments and suggestions regarding content to *FSISUpdate@fsis.usda.gov*. If you aren't regularly receiving the *Constituent Update*, you can sign up for it at *http://www.fsis.usda.gov/wps/portal/fsis/newsroom/meetings/newsletters/constituent-updates*.

FSIS *Constituent Update* is prepared by the Congressional and Public Affairs Staff
Office of Public Affairs
and Consumer Education

Assistant Administrator
Carol Blake

Deputy Assistant Administrator
Aaron Lavallee

Editorial Staff

Editor
Veronika Medina

Assistant Editor
Josh Stull

Content & Technical Review Committee
Kristen Booze
Maria Machuca
Katherine Scheidt
Brittany Woodland

Insider Threats: Are you Prepared?

What is an insider threat?

Malicious insiders can take advantage of trusted access to facilities, products, information systems, data or personal relationships to inflict damage to a company or individuals. An insider threat can be defined as a current or former employee, contractor or business partner with authorized access to systems and facilities and has intentionally used that access to negatively affect the company. In the past, insider threats were mostly associated with information security. While attacks in the cyber realm continue to increase, there is also a need for continued vigilance within the food industry to protect against insider threats associated with foreign and domestic extremists or disgruntled employees. Consequences of an attack by someone with inside access may include:

- Cyber security breaches
- Theft of intellectual property or other important company information
- Embarrassment/damage to your company brand
- Tampering and/or adulteration of product which may negatively impact public health or the economic livelihood of the company
- Workplace violence
- Terrorist attacks

How can you detect and report an insider threat?

Individuals who pose an inside threat can go unnoticed for months or years. According to the Federal Bureau of Investigation, there are a number of personal factors and behavioral indicators that could be indicative of a threat posed by an insider:

Characteristics/Behaviors of Insiders who may pose a threat to your organization (not all-inclusive)

- Greed or financial need
- Anger/revenge
- Problems at work
- Identification with extremist groups/ideologies
- Divided loyalty
- Adventure/thrill
- Vulnerability to blackmail
- Compulsive and destructive behavior
- Family problems
- Takes proprietary materials/information home (without need or authorization)
- Interest in matters outside the scope of their duties
- Remotely accesses the computer network while on vacation, sick leave, or at other odd times
- Works odd hours without authorization
- Unreported foreign contacts
- Short trips to foreign countries for unexplained or strange reasons
- Unexplained affluence
- Overwhelmed by life crises or career disappointments
- Concern that they are being investigated

If you, or individuals within your organization, observe suspicious types of behavior, it is important to say something. The Department of Homeland Security's (DHS) "If you See Something, Say Something™" campaign is a good avenue for encouraging individuals to report suspicious activity to appropriate authorities, whether that be company supervisors, security personnel, or state and local law enforcement. For additional information on the "If you See Something, Say Something™" campaign, please visit *http://www.dhs.gov/see-something-say-something*.

Mitigating insider threats:

Being prepared for insider threats can go a long way to reduce the potential impact to your establishment.

Continue on page 4

Food Recalls and Alerts

Stay up-to-date on FSIS' food recall alerts by visiting FSIS' Current Recalls and Alerts Web page at *http://www.fsis.usda.gov/recalls*.

You can also receive e-mail notifications when public health alerts and recalls are issued. Register at *http://www.fsis.usda.gov/subscribe*.

...Insider Threats

Continued from Page 3

A number of tools and resources are available to help companies mitigate threats from insiders, including:

• **Implementing a functional food defense plan** - A functional food defense plan can help industry identify mitigation measures to protect against insider threats, including conducting background checks on employees and individuals with access to company resources, password protecting computers and access to networks, and implementing employee identification systems, to name a few. FSIS' Food Defense Risk Mitigation Tool is available to help industry identify security measures that can be implemented, as part of a functional food defense plan, to protect against insider threats. For additional information on functional food defense plans and to access the Food Defense Risk Mitigation Tool, please visit *www.fsis.usda.gov/FoodDefense.*

• **Training employees to identify and report suspicious activity surrounding insider threats (DHS, 2014):** The following exercises and courses can be used to train employees on insider threats:

- FSIS Food Defense and Recall Preparedness Scenario-Based Exercise Tool provides commodity-specific exercises to introduce employees to an insider threat scenario. *www.fsis.usda.gov/FoodDefense*.
- Protecting Critical Infrastructure Against Insider Threats - IS-915 (DHS) - free online course to provide guidance to critical infrastructure employees (including the food industry) on how to identify and take action against insider threats. *http://www.training.fema.gov/is/courseoverview.aspx?code=IS-915.*
- Insider Threat Awareness Toolkit (Department of Defense) – free online set of resources that focus on insider threat awareness as an essential component of a comprehensive security program. *http://www.cdse.edu/toolkits/insider/awareness.html.*
- Training and awareness films addressing insider threats – (National Counterintelligence and Security Center). *http://www.ncsc.gov/industry/video/index.html.*

Questions or requests for additional information on insider threats or other food defense topics can be directed to the FSIS Food Defense Assessment Staff (FoodDefense@fsis.usda.gov).

Update: FSIS Testing for *E. coli*

FSIS posts bi-weekly updates of the Agency's raw ground beef *E. coli* sampling program. Included are testing results of raw ground beef component samples for *E. coli* O157:H7 and STECs from FSIS routine and follow-up sampling programs. Also featured is data for non-O157 STECs by each non-O157 STEC serogroup.

Between June 4, 2012 and Jan.10, 2016, FSIS laboratory services analyzed a total of 12,010 beef trim samples (10,281 domestic and 1,729 imported), 3,098 routine follow-up samples (2,984 domestic and 114 imported), and 326 non-routine follow-up/traceback samples. There were 145 positive samples; 80 domestic trim samples, four imported trim samples, 57 domestic follow-up samples, and four non-routine follow-up/traceback samples. To date, three samples have been positive for both O157:H7 and at least one non-O157 STEC strain, and eight samples have been positive for two different non-O157 O-groups.

To review testing results, visit the *E. coli* data tables at *http://www.fsis.usda.gov/wps/portal/fsis/topics/data-collection-and-reports/microbiology/ec/.*

FSIS Policy Updates

FSIS notices and directives on public health and regulatory issues are available at *http://www.fsis.usda.gov/wps/portal/fsis/topics/regulations*. The following policies were recently issued:

Docket No. FSIS-2015-0044 - Codex Alimentarius Commission - Meeting of the Codex Committee on Food Additives